IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for securely confirming performance of task by a peer in a peer-to-peer network, comprising:

broadcasting a request over the network by a requesting peer for a task with respect to a remote non-local backend server;

receiving a response to the request containing a local alias URL, the local alias URL pointing to a local upload directory for a vendor HTTP service server residing ~~a destination~~ on a responding server node, where the vendor HTTP service server uploads files from the local upload directory to the remote non-local backend server;

forwarding the task to the local alias URL for performance of the task by the responding server node;

verifying a digital signature of any receipt packet received from the responding server node to ensure that the receipt packet is from the remote non-local backend server; and

awaiting a maximum upload receipt time period for receiving the receipt packet;

wherein the maximum upload receipt time period is set based on a frequency of which an uploading service at the responding server node performs an upload, a size of a file being uploaded, and a transmission speed;

wherein the server node is placed in a black list of the requesting peer if said verifying is unsuccessful;

wherein, after said receiving, a message is broadcasted indicating that the requesting peer has located the responding server node;

wherein the task is an uploading task and wherein said forwarding the task to the local alias URL includes forwarding a file to be uploaded to the remote non-local backend server, and uniquely identifying the forwarded file.

2. (Cancelled)

3. (Cancelled)

4. (Previously Presented) A method for securely confirming performance of task by a peer of claim 1, further comprising placing the server node in the black list of the requesting peer if a receipt packet fails to arrive within said maximum upload receipt time period.

5. (Cancelled)

6. (Original) A method for securely confirming performance of task by a peer of claim 1, wherein the digitally signed response is signed by a 1024-bit VeriSign digital certificate.

7. (Cancelled)

8. (Cancelled)

9. (Currently Amended) A computer program product for securely confirming performance of task by a peer in a peer-to-peer network, comprising:

computer code of a requesting peer that broadcasts a request over the network for a task with respect to a remote non-local backend server;

computer code that receives a response to the request, the response containing a local alias URL, the local alias URL pointing to a local upload directory for a vendor HTTP service server residing ~~a destination~~ on a

responding server node, where the vendor HTTP service server uploads files from the local upload directory to the remote non-local backend server;

computer code that forwards the task to the local alias URL for performance of the task by the responding server node; and

computer code that verifies a digital signature of any receipt packet received from the responding server node to ensure that the receipt packet is from the remote non-local backend server;

computer code that awaits a maximum upload receipt time period for receiving the receipt packet; and

a computer readable medium that stores said computer codes;

wherein the maximum upload receipt time period is set based on a frequency of which an uploading service at the responding server node performs an upload, a size of a file being uploaded, and a transmission speed;

wherein the server node is placed in a black list of the requesting peer if said verifying is unsuccessful;

wherein, after said receiving, a message is broadcasted indicating that the requesting peer has located the responding server node;

wherein the task is an uploading task and wherein said forwarding the task to the local alias URL includes forwarding a file to be uploaded to the remote non-local backend server, and uniquely identifying the forwarded file.

10. (Cancelled)

11. (Cancelled)

12. (Previously Presented) A computer program product for securely confirming performance of task by a peer of claim 9, further comprising computer code that places the server node in the black list of the requesting peer if a receipt packet fails to arrive within said maximum upload receipt time period.

13. (Cancelled)

14. (Original) A computer program product for securely confirming performance of task by a peer of claim 9, wherein the digitally signed response is signed by a 1024-bit VeriSign digital certificate.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Previously Presented) A method for securely confirming performance of task by a peer of claim 1, wherein the method reduces a number of service clients that have to obtain files via the Internet.

19. (Previously Presented) A method for securely confirming performance of task by a peer of claim 1, wherein the task includes updating security files.

20. (Previously Presented) A method for securely confirming performance of task by a peer of claim 19, wherein the security files include firewall files and anti-virus application files.

21. (Currently Amended) A system for securely confirming performance of task by a peer in a peer-to-peer network, comprising:

means for broadcasting a request over the network by a requesting peer for a task with respect to a remote non-local backend server;

means for receiving a response to the request containing a local alias URL, the local alias URL pointing to a local upload directory for a vendor HTTP service server residing ~~a destination~~ on a responding server node, where the vendor HTTP service server uploads files from the local upload directory to the remote non-local backend server;

means for forwarding the task to the local alias URL for performance of the task by the responding server node;

means for verifying a digital signature of any receipt packet received from the responding server node to ensure that the receipt packet is from the remote non-local backend server; and

means for awaiting a maximum upload receipt time period for receiving the receipt packet;

wherein the maximum upload receipt time period is set based on a frequency of which an uploading service at the responding server node performs an upload, a size of a file being uploaded, and a transmission speed;

wherein the server node is placed in a black list of the requesting peer if said verifying is unsuccessful;

wherein, after said receiving, a message is broadcasted indicating that the requesting peer has located the responding server node;

wherein the task is an uploading task and wherein said forwarding the task to the local alias URL includes forwarding a file to be uploaded to the remote non-local backend server, and uniquely identifying the forwarded file.

22. (New) A method for securely confirming performance of task by a peer of claim 1, wherein the packet includes the following format: <service type = "X" version = "X" ID = "X" method = "X" href = http://X acceptprotoco = "X"/>.

23. (New) A method for securely confirming performance of task by a peer of claim 1, wherein the files each include an XML file.

24. (New) A computer program product for securely confirming performance of task by a peer of claim 9, wherein the packet includes the following format: <service type = "X" version = "X" ID = "X" method = "X" href = http://X acceptprotoco = "X"/>.

25. (New) A computer program product for securely confirming performance of task by a peer of claim 9, wherein the files each include an XML file.

26. (New) A system for securely confirming performance of task by a peer of claim 21, wherein the packet includes the following format: <service type = "X" version = "X" ID = "X" method = "X" href = http://X acceptprotoco = "X"/>.

27. (New) A system for securely confirming performance of task by a peer of claim 21, wherein the files each include an XML file.